

1 **BRADLEY/GROMBACHER, LLP**

2 Marcus J. Bradley, Esq. (SBN 174156)

3 Kiley L. Grombacher, Esq. (SBN 245960)

4 Lirit A. King, Esq. (SBN 252521)

5 31365 Oak Crest Drive, Suite 240

6 Westlake Village, California 91361

7 Telephone: (805) 270-7100

8 Facsimile: (805) 270-7589

9 E-Mail: [mbradley@bradleygrombacher.com](mailto:mbradley@bradleygrombacher.com)

10 [kgrombacher@bradleygrombacher.com](mailto:kgrombacher@bradleygrombacher.com)

11 [lking@bradleygrombacher.com](mailto:lking@bradleygrombacher.com)

12 *Attorneys for Plaintiffs*

13 (Additional counsel listed on following page)

14 **UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA  
SAN FRANCISCO DIVISION**

15 JUAN FLORES-MENDEZ, an individual and  
16 AMBER COLLINS, an individual, and on  
behalf of classes of similarly situated  
17 individuals,

18 Plaintiffs,

19 v.

20 ZOOSK, INC., a Delaware corporation,

21 Defendant.

22 **CASE NO: 3:20-cv-04929-WHA**

23 **PLAINTIFFS' THIRD AMENDED CLASS  
ACTION COMPLAINT FOR:**

24 **1. NEGLIGENCE; AND**

25 **2. VIOLATION OF CALIFORNIA'S  
UNFAIR COMPETITION LAW, CAL.  
BUS. & PROF. CODE § 17200, ET SEQ.**

26 **DEMAND FOR A JURY TRIAL**

1           **BRADLEY/GROMBACHER, LLP**

2           Robert N. Fisher (SBN 302919)  
3           477 Madison Avenue, Suite 6000  
4           New York, NY 10022  
5           Telephone: (805) 270-7100  
6           E-Mail: [rfisher@bradleygrombacher.com](mailto:rfisher@bradleygrombacher.com)

7           **CROSNER LEGAL P.C.**

8           Zachary M. Crosner (SBN 272295)  
9           Michael R. Crosner (SBN 41299)  
10          433 N. Camden Dr., Suite 400  
11          Beverly Hills, CA 90210  
12          Telephone: (310) 496-4818  
13          Facsimile: (310) 510-6429  
14          Email: [zach@crosnerlegal.com](mailto:zach@crosnerlegal.com)  
15          mike@crosnerlegal.com

16          **MORGAN & MORGAN  
17          COMPLEX LITIGATION GROUP**

18          John A. Yanchunis (*admitted pro hac vice*)  
19          Ryan McGee (*admitted pro hac vice*)  
20          201 N Franklin St., 7th Floor  
21          Tampa, FL 33602  
22          Telephone: (813) 223-5505  
23          Email: [jyanchunis@forthepeople.com](mailto:jyanchunis@forthepeople.com)  
24                    [rmcghee@forthepeople.com](mailto:rmcghee@forthepeople.com)

25          *Attorneys for Plaintiffs*

26

27

28

1 Plaintiffs Juan Flores-Mendez, and Amber Collins, individually and on behalf of classes of  
 2 similarly situated individuals (defined below), bring this action against Defendant Zoosk, Inc.  
 3 (“Zoosk”). Plaintiffs and their counsel believe that reasonable discovery will provide additional  
 4 evidentiary support for the allegations herein.

5 **INTRODUCTION**

6 1. Zoosk is a self-touted “leading online data company” with over 35 million  
 7 members.<sup>1</sup> Zoosk employs its proprietary Behavioral Matchmaking™ technology to leverage the  
 8 data generated by users on the platform and deliver matches which are predicted to result in “mutual  
 9 attraction.”<sup>2</sup>

10 2. To engage Defendant’s online matchmaking services, customers create and populate  
 11 user profiles with personally identifiable information (“PII”) such as first and last name, email  
 12 address, password, home address, telephone number, and payment card information. Zoosk  
 13 customers trust that their PII will be maintained in a secure manner and kept from unauthorized  
 14 disclosure to third parties as outlined in Zoosk’s Privacy Policy.<sup>3</sup>

15 3. Zoosk customers also have the option of paying for a premium subscription service,  
 16 which costs \$29.99 for a single month, or \$12.49 per month for a six-month period. Plaintiff Juan  
 17 Flores-Mendez paid for this subscription before the Data Breach was announced.

18 4. Over the first two weeks of May, a group calling itself the “ShinyHunters” went on  
 19 a hacking rampage and subsequently set out to hawk what it claimed to be close to 200 million  
 20 stolen records from at least 13 companies, including “Zoosk.”<sup>4</sup> Indeed, of all the companies  
 21 targeted, Zoosk had the largest breach, as the cybercriminals grabbed 30 million user records.<sup>5</sup>

---

22  
 23 <sup>1</sup> <https://about.zoosk.com/en/about/>

24 <sup>2</sup> <https://www.sec.gov/Archives/edgar/data/1438964/000119312514146003/d672159ds1.htm>

25 <sup>3</sup> [https://docviewer.zoosk.com/legal-privacy-en\\_eu.html](https://docviewer.zoosk.com/legal-privacy-en_eu.html)

26 <sup>4</sup> <https://www.wired.com/story/shinyhunters-hacking-group-data-breach-spree/>

27 <sup>5</sup> <https://www.dailymail.co.uk/sciencetech/article-8308167/Hacker-group-ShinyHunters-sells-73-MILLION-user-records-dark-web.html>

1       5. An entity claiming to be a member of ShinyHunters said in an instant message  
 2 conversation with WIRED that it is “not too hard” to breach so many organizations.<sup>6</sup>

3       6. According to its notice to affected customers, on May 11, 2020 Zoosk “learned that  
 4 an unknown third party claimed to have accessed certain Zoosk member information” (the “Data  
 5 Breach.”).

6       7. Over three weeks later, and more than four weeks after the Data Breach occurred,  
 7 Zoosk notified affected customers that their PII had been disclosed to unauthorized and malicious  
 8 third parties.

9       8. To date, Zoosk has acknowledged that the customer information disclosed in the  
 10 Data Breach included a combination of the following PII:

- 11           • name;
- 12           • email address;
- 13           • date of birth;
- 14           • generalized demographical information;
- 15           • gender;
- 16           • gender search preferences; and
- 17           • password information.

18       9. Zoosk’s Notice of Data Security Event was sent via email on May 28, 2020,  
 19 including a phone number for customer inquiries, as required by Cal. Civ. Code section 1798.82(a).  
 20 Section 1798.82(a) requires businesses to notify “any California resident (1) whose unencrypted  
 21 personal information was, or is reasonably believed to have been, acquired by an unauthorized  
 22 person, or, (2) whose encrypted personal information was, or is reasonably believed to have been,  
 23 acquired by an unauthorized person and the encryption key or security credential was, or is  
 24 reasonably believed to have been, acquired by an unauthorized person and the person or business  
 25 that owns or licenses the encrypted information has a reasonable belief that the encryption key or  
 26 security credential could render that personal information readable or usable. The disclosure shall

---

27       6 <https://www.wired.com/story/shinyhunters-hacking-group-data-breach-spree/>

1 be made in the most expedient time possible and without unreasonable delay, consistent with the  
 2 legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to  
 3 determine the scope of the breach and restore the reasonable integrity of the data system.”

4       10. The Zoosk customer PII disclosed in the Data Breach is protected by the California  
 5 Consumer Privacy Act of 2018 (“CCPA”), which went into effect on January 1, 2020. For purposes  
 6 of the CCPA, “personal information” is defined as an individual’s first name or first initial and his  
 7 or her last name in combination with any one or more of the following data elements, when either  
 8 the name or the data elements are not encrypted or redacted: (1) social security number; (2) driver’s  
 9 license number or California ID card number; (3) account number or credit or debit card number, in  
 10 combination with any required security code, access code or password that would permit access to  
 11 an individual’s financial account; (4) medical information; and/or (5) health insurance information.

12       11. Alternatively, protected PII includes “A username or email address in combination  
 13 with a password or security questions and answer that would permit access to an online account.”

14       12. According to Zoosk’s notice to affected customers, the PII subjected to unauthorized  
 15 access and exfiltration, theft or disclosure in the Data Breach includes (among other things): (i)  
 16 customers’ unencrypted and unredacted name, and (ii) an email address that serves as an account  
 17 login/account number, and (iii) password (although not confirmed at the time of the notice).  
 18 In combination, those pieces of PII could permit access to other accounts using similar passwords,  
 19 including financial accounts.

20       13. Zoosk has failed to maintain reasonable security controls and systems appropriate  
 21 for the nature of the PII it maintains as required by the CCPA and other common and statutory laws.

22       14. Zoosk also failed to maintain proper measures to detect hacking and intrusion.  
 23 According to its notice to affected customers, Zoosk did not learn that its customer records were  
 24 stolen until the hack was publicly reported. As explained below, Zoosk should have had breach  
 25 detection protocols in place. If it had, it could have learned of the breach and alerted customers  
 26 much sooner.

27

28

1       15. Because (i) Zoosk has failed to maintain reasonable security measures, and (ii) the  
 2 names that Zoosk disclosed in combination with emails and passwords were unredacted and  
 3 unencrypted, Zoosk has breached its legal duties and obligations to Plaintiffs and Class Members.

4       16. Zoosk claims its “investigation remains ongoing,” is “taking several steps to monitor  
 5 systems and enhance our existing security measures and processes,” but the viewing, theft, and  
 6 attempted sale of California consumers’ PII on the dark web has already occurred and cannot be  
 7 cured.

8       17. Defendant disregarded Plaintiffs’ and Class members’ privacy rights in the PII by,  
 9 among other things, (i) failing to implement reasonable security safeguards to prevent or timely  
 10 detect the Data Breach; (ii) failing to disclose to customers that it did not implement such reasonable  
 11 security safeguards; and (iii) failing to provide sufficiently prompt, thorough, and accurate notice  
 12 and information concerning the Data Breach.

13       18. As a result of the Data Breach, Plaintiffs and the Classes have been injured in several  
 14 ways. Plaintiffs and Class members (i) now know or should know that their PII was hacked and put  
 15 up for sale on the dark web for purchase by malicious actors; (ii) face an imminent and ongoing  
 16 risk of identity theft and similar cybercrimes; (iii) have expended and will continue to expend time  
 17 and money to protect against cybercrimes; (iv) have lost value in their PII; and (v) did not receive  
 18 the benefit of their bargain with Defendant regarding data privacy.

19       19. Plaintiffs and Class members are therefore (i) entitled to actual damages under the  
 20 CCPA and other laws, (ii) have incurred actual and concrete damages as a result of the unauthorized  
 21 sale of their PII to malicious actors on the dark web, and (iii) face ongoing risks of disclosure of  
 22 their PII in subsequent data breaches because Defendant has not demonstrated that it has  
 23 implemented reasonable security systems and procedures. Plaintiffs and Class members have a  
 24 significant interest in the protection and safe storage of their PII. They are therefore entitled to  
 25 declaratory, injunctive, and other equitable relief necessary to protect their PII. This includes, but  
 26 is not limited to, an order compelling Defendant to adopt reasonable security procedures and  
 27 practices to safeguard customers’ PII and prevent future data breaches.

**JURISDICTION AND VENUE**

20. This Court has jurisdiction over this action pursuant to the Class Action Fairness  
 Act (“CAFA”), 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds  
 \$5,000,000, exclusive of interests and costs, there are more than 100 class members, and one or  
 more members of the Classes are residents of a different state than Defendant Zoosk. The Court also  
 has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1337.

21. This Court has personal jurisdiction over Defendant because it has continuous and  
 systematic contacts with and conduct substantial business in the State of California and this District.  
 Defendant Zoosk maintains its principal place of business in this District and has continuous and  
 systematic contacts with and conducts substantial business in the State of California and this District.

22. Venue is proper in this District pursuant to 28 U.S.C. § 1331(b). A substantial part  
 of the events giving rise to these claims took place in this District, numerous Class members reside  
 in this District and were therefore harmed in this District.

**INTRADISTRICT ASSIGNMENT**

23. This action is properly assigned to the San Francisco Division of this District  
 pursuant to N.D. Cal. L.R. 3-2 because a substantial part of the events or omissions giving rise to  
 Plaintiffs’ claims arose in the counties served by the San Francisco Division. Zoosk is  
 headquartered in this Division and conducts substantial business in the counties served by this  
 Division, has marketed, advertised, sold, and collected contact information from consumers in this  
 District, and has caused harm to Class members residing in those counties.

**PARTIES**

24. Plaintiff Juan Flores-Mendez (“Plaintiff Flores-Mendez”) is a permanent resident  
 of, California. Plaintiff Flores-Mendez created a user profile on Zoosk’s website in or about 2015  
 or 2016. Plaintiff Flores-Mendez entrusted Zoosk with their PII. On May 28, 2020, Plaintiff  
 Flores-Mendez received a notice in the mail from Zoosk notifying him that his PII had been  
 accessed by malicious third parties without authorization. Because of the Data Breach, he has  
 continuously monitored his various accounts to detect misuse of his PII and will continue to expend

1 time to protect against fraudulent use or sale of his PII.

2 25. As a result of the notice, Plaintiff Flores-Mendez spent time dealing with the  
 3 consequences of the data breach, which includes time spent reviewing the account compromised by  
 4 the breach, contacting his credit card company, reviewing her credit report for suspicious activity,  
 5 putting fraud alerts on his credit report, exploring credit monitoring options, and self-monitoring his  
 6 accounts.

7 26. Knowing that the hacker stole his PII, and that his PII may be available for sale on  
 8 the dark web, has caused Plaintiff Flores-Mendez anxiety. Plaintiff Flores-Mendez is now greatly  
 9 concerned about credit card theft and identity theft in general. This breach has given Plaintiff Flores-  
 10 Mendez hesitation about utilizing online websites.

11 27. Plaintiff Amber Collins (“Plaintiff Collins”) is a permanent resident of Simi Valley,  
 12 California. Plaintiff Collins created a user profile on Zoosk’s website in or about 2016. Plaintiff  
 13 Collins entrusted Zoosk with their PII. During the first week of June, 2020, an alert notice from  
 14 Credit Karma notifying her of the breach of her Zoosk account. Because of the Data Breach, Plaintiff  
 15 Collins has continuously monitored her various accounts to detect misuse of her PII and will  
 16 continue to expend time to protect against fraudulent use or sale of her PII.

17 28. As a result of the notice, Plaintiff Collins spent time dealing with the consequences  
 18 of the data breach, which includes time spent reviewing the account compromised by the breach,  
 19 contacting her credit card company, signing up for credit monitoring options, reviewing her credit  
 20 report for suspicious activity, putting fraud alerts on her credit reports, and self-monitoring her  
 21 accounts.

22 29. Knowing that the hacker stole her PII, and that her PII may be available for sale on  
 23 the dark web, has caused Plaintiff Collins anxiety. Plaintiff Collins is now greatly concerned about  
 24 credit card theft and identity theft in general. This breach has given Plaintiff Collins has hesitation  
 25 about Zoosk and other online websites.

26 30. Defendant Zoosk is a for-profit Delaware corporation and maintains a headquarters  
 27 and principal place of business in San Francisco, California. The Zoosk app, available in more than  
 28

1 80 countries, is a free download, but charges users who want to send messages and chat with other  
2 subscribers, similar to Match. Zoosk has gross revenues in excess of \$25 million as adjusted. Zoosk  
3 was acquired by Berlin-based Spark Networks in July 2019. The deal valued Zoosk at approximately  
4 \$258 million.

5       31. According to data from Sensor Tower, Zoosk has generated worldwide in-app  
6 revenue of \$250 million and has seen 38 million downloads since January 2014. Half of those  
7 downloads (19 million) are from the U.S., which also accounts for \$165 million (66%) of the  
8 revenue. In Quarter one of 2019, Zoosk had revenue of \$13 million.

## **FACTUAL BACKGROUND**

## **10 | Defendant's Relevant Privacy Policies**

11           32. Personal data must be provided in order for consumers to use the service provided by  
12 Zoosk.

13        33. Zoosk's Privacy Policy is available on its website and provides customers with terms  
14 and conditions regarding the treatment of their PII. For example, it states:

**15** When you register, use or subscribe to any of our Services or take part in any interactive  
**16** features of the Services (such as any contests, games, promotions, quizzes, surveys, research or other services or features), we may collect a variety of information, including:

- a. Contact Information such as your name, email address, phone number, and address (“Contact Information”);
  - b. Sensitive Information such as race, ethnicity, sexual preferences and experiences, political affiliation, religious affiliation, union memberships, or any biometric information you provide through the use of our Services (your “Sensitive Personal Data”);
  - c. Other Information such as birth date, videos, passwords, billing information, credit card information, demographic information, place of work or education, your personal interests and background, gender, age, dating age range preference, physical characteristics, personal description, life experiences, geographic location, your photos and any information derived from them, and any other information you share with the Services. We may collect billing or payments information if you engage with a paid Service.<sup>7</sup>

<sup>7</sup> <https://docviewer.zoosk.com/legal-privacy-en.html>

1       34. Additionally, Zoosk collects information about:<sup>8</sup>

- 2             • How consumers use the service (*i.e.*, pages and profiles viewed);  
3             • Content users upload (*i.e.*, time, date and place information for photos uploaded to the  
4             site as well as the identity of those to whom the photos are shared);  
5             • Information about your devices (*i.e.*, model and manufacturer, mobile carrier, phone  
6             number, other apps downloaded, IP address, browser type, Internet service provider,  
7             platform type, the site from which you came and the site to which you are going when  
8             you leave our website);  
9             • Communications (sent directly to Zoosk or comments made by users on third-party  
10            services such as Twitter Instagram, Pinterest, Tumblr and YouTube);  
11             • Information taken from social networking sites (*i.e.* IP address, browser type, Internet  
12            service provider, platform type, the site from which you came and the site to which  
13            you are going when you leave our website, date and time stamp and one or more  
14            cookies that may uniquely identify your browser or your account);  
15             • Location data;  
16             • User's address book contact information; and  
17             • Aggregated data.

18       35. When Plaintiff Flores-Mendez signed up for his account with Zoosk in or about 2015 or  
19       2016, Zoosk's then-current Privacy Policy explained, in relevant part "how information about [consumers]  
20       or associated with [consumers]" ('Personal Information') is collected, used and disclosed by Zoosk,"  
21       including when Plaintiff Flores-Mendez and other users "use[d Zoosk's] services through [Zoosk's]  
22       websites linked to th[e Privacy] Policy, as well as [Zoosk's] products and applications (including Zoosk's  
23       mobile applications, downloadable products and applications and pages operated by Zoosk on social  
24       networking sites and other platforms) (collectively, the 'Services.'")<sup>9</sup>

25  
26       

---

<sup>8</sup> *Id.*

27       <sup>9</sup> See Zoosk Terms and Policies, Privacy Policy (July 8, 2016) available at:  
28       <https://web.archive.org/web/20151117004210/https://www.zoosk.com/en/privacy?from=footer>

1       36. In Section 1 of the Privacy Policy, Zoosk further detailed how consumers' personal  
 2 information was collected, including: information that consumers provide; how consumers interact  
 3 with Zoosk's Services and uploaded content; information that Zoosk automatically collects;  
 4 information collected through Zoosk's use of cookies and similar technologies; consumers'  
 5 communications; third-party social networking sites (when enabled); location data; and consumers'  
 6 address books (when provided).<sup>10</sup>

7       37. In Section 3 of the Privacy Policy, Zoosk further detailed how consumers'  
 8 information was shared with third parties, representing that Zoosk's Services:

9             [A]llow you to share information about yourself with other individuals and other  
 10 companies, including other users and potential users of the Services and third-party  
 11 Social Networking Sites. *Consider your own privacy and personal safety when*  
*sharing your information with anyone, including information you share through your*  
*profile*, as profiles as profiles include basic information that was provided at  
 12 registration, information provided through a Social Networking Site, and may include  
 13 other information added by you or your friends (for example, your religion, ethnicity  
 14 and physical characteristics), as well as information about your use of the Service  
 (for example, whether you were recently logged in to Zoosk).<sup>11</sup>

15       38. In Section 3 of the Privacy Policy, Zoosk lists the third parties to which this  
 16 information *may* be shared, which includes third parties to assist Zoosk in carrying out its Services;  
 17 business partners; mergers or business transactions; court orders; or to "detect, prevent or otherwise  
 18 address criminal (including fraud or stalking), security or technical issues."<sup>12</sup>

19       39. Indeed, also in Section 3 of the Privacy Policy, Zoosk tacitly acknowledged that it  
 20 collects both sensitive and non-sensitive information on consumers, stating that it "may also share  
 21 information with others that is not personal information or that is in an aggregated or anonymous  
 22 form that does not reasonably identify you directly as an individual."<sup>13</sup>

---

23  
 24 <sup>10</sup> *Id.*

25 <sup>11</sup> *Id.* (emphasis added).

26 <sup>12</sup> *Id.* (emphasis added).

27 <sup>13</sup> *Id.*

1       40. Moreover, in Section 5 of the Privacy Policy, Zoosk reiterated its commitment to  
 2 security, “reserv[ing] the right to maintain and store any information or other data Zoosk reasonably  
 3 believes in its sole discretion that such action is required . . . for the detection or prevention of  
 4 criminal or other unlawful activity . . .”<sup>14</sup>

5       41. In Section 6 of the Privacy Policy, Zoosk also committed to taking “reasonable  
 6 measures to help protect [consumers’] information in an effort to prevent loss, misuse, and  
 7 unauthorized access, disclosure, alteration or destruction and to treat it in accordance with th[e  
 8 Privacy] Policy.”<sup>15</sup> Although Zoosk opined that “[n]o method of electronic transmission or storage  
 9 is 100% secure,”<sup>16</sup> such a statement cannot absolve Zoosk of its responsibility of taking the  
 10 “reasonable measures” Zoosk committed to taking to ensure the security of consumers’ data in  
 11 Sections 1, 2, 3, 4, and 5 of the Privacy Policy, *supra* ¶¶ 36–40.

12       42. Zoosk bound all parties, including Plaintiffs and Class Members alike, to the Privacy  
 13 Policy, stating that “By registering, using or subscribing to the Services, you confirm that you have  
 14 *read and consent to*” the portions of the Privacy Policy described, *supra* ¶¶ 36–41 (emphasis added).

15       43. Upon information and belief, and reasonable investigation of counsel, the  
 16 representations in Zoosk’s Privacy Policy were not changed between October 7, 2013, and when  
 17 Plaintiff Flores-Mendez signed up for and began using Zoosk’s services, including through Zoosk’s  
 18 website and Zoosk’s mobile application.<sup>17</sup>

19       44. Upon information and belief, and reasonable investigation of counsel, the  
 20 representations from Zoosk’s Privacy Policy were not materially changed in subsequent revisions  
 21 during the Class Period until March 27, 2020—the previous Privacy Policy “confirmed that  
 22 [consumers] ha[d] read and consent[ed] to” how information was collected, how information was  
 23

24       <sup>14</sup> *Id.*

25       <sup>15</sup> *Id.*

26       <sup>16</sup> *Id.*

27       <sup>17</sup> See *id.* (Section 11, stating “This Policy was last revised on October 7, 2013.”)

1 used, how information was shared *and not shared* with third parties, the used for the prevention of  
 2 criminal or other unlawful activity.”<sup>18</sup>

3       45. Because Zoosk’s then-current Privacy Policy presumed that any consumer who used  
 4 Zoosk’s Services read the Privacy Policy, and also compelled consent of those consumers through  
 5 use of the Services, Zoosk was bound by those promises to Plaintiffs and Class Members.

6       46. With these binding terms in place, Plaintiff Flores-Mendez continued to pay for  
 7 Zoosk’s Services, and also continued to provide his PII, which included: 1) his use of the Services,  
 8 such as pages and profiles viewed); 2) information about his devices used to access Zoosk’s  
 9 Services, such as the model and manufacturer, mobile carrier, phone number, other apps  
 10 downloaded, IP address, browser type, ISP, operating system, and sites visited before and after  
 11 Zoosk; 3) communications with Zoosk; 4) location data; and 5) other data that Zoosk aggregates.

12       47. Had Zoosk properly notified consumers that its security was inadequate and that it  
 13 was not complying with its Privacy Policy, Plaintiff Flores-Mendez would have ceased use of the  
 14 Zoosk Services, ceased providing Zoosk with his sensitive and confidential PII, and ceased paying  
 15 for the Zoosk Services.

#### **Zoosk Uses PII to Maximize Its Profits and For Marketing**

17       48. Zoosk’s Privacy Policy reveals the significant benefit Zoosk derives from collecting  
 18 and maintaining its customers PII. In addition to the uses listed above, Zoosk:

- 19           • Permits third party advertising networks, social media companies and other third  
 20           party businesses to collect PII (including Internet/Network Information,  
 21           Commercial Information, and Inferences) directly from consumer’s browsers or  
 22           devices through cookies or tracking technologies. These third parties use this  
 23           information for the purposes of serving ads, for ad campaign measurement and

---

25       <sup>18</sup> See Zoosk Terms and Policies, Privacy Policy (March 3, 2020) available at:  
 26           <https://web.archive.org/web/20200303020958/https://docviewer.zoosk.com/legal-privacy-en.html>,  
 27           stating in Section 13 that the last revision date was September 7, 2016; Cf Zoosk Privacy Policy  
 28           (April 28, 2020) available at: <https://web.archive.org/web/20200428065639/https://docviewer.zoosk.com/legal-privacy-en.html> (Section 7 noting last revision of March 27, 2020).

1           analytics, and may sell that information to other businesses for advertising and  
 2           other purposes;

- 3           • Uses PII to facilitate users' purchase of subscriptions and premium add-ons;
- 4           • Shares PII with promotional partners to provide contests and sweepstakes or  
             other joint promotional activities;
- 5           • May utilize PII in connection with any company transaction, such as a merger,  
             sales of assets or shares, reorganization, financing, change of control or  
             acquisition of all or a portion of our business by another company or third party  
             or in the event of bankruptcy, dissolution, divestiture or any related or similar  
             proceedings for marketing and advertising purposes; and
- 6           • Uses PII to monitor, improve, and develop its products and services.

12 **Zoosk Failed to Take Reasonable Steps to Protect User Data**

13         49. By collecting, using, and deriving significant benefit from customers' PII, Zoosk had  
 14         a legal duty to take reasonable steps to protect this information from disclosure.

15         50. As discussed below, Defendant also had a legal duty to take reasonable steps to  
 16         protect customers' PII under applicable federal and state statutes, including Section 5 of the Federal  
 17         Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which is further defined by federal and state  
 18         guidelines and industry norms.

19         51. Defendant breached its duties by failing to implement reasonable safeguards to  
 20         ensure Plaintiffs' and Class members' PII was adequately protected. As a direct and proximate result  
 21         of this breach of duty, the Data Breach occurred, and Plaintiffs and Class members were harmed.  
 22         Plaintiffs and Class members did not consent to having their PII disclosed to any third-party, much  
 23         less a malicious hacker who would sell it on the dark web.

24         52. The Data Breach was a reasonably foreseeable consequence of Defendant's  
 25         inadequate security systems. Defendant Zoosk, is valued at \$258 Million Dollars, has the resources  
 26         to implement reasonable security systems to prevent or limit damage from data breaches. Even so,  
 27         it failed to properly invest in its data security. If Zoosk had implemented reasonable data security

1 systems and procedures (*i.e.*, followed guidelines from industry experts and state and federal  
 2 governments), then it likely could have prevented hackers from infiltrating its systems and accessing  
 3 its customers' PII.

4 **Zoosk's Failure to Take Reasonable Steps to Protect User Data Resulted in a Massive Data**  
**Breach**

5       53.     A data breach is any incident where confidential or sensitive information has been  
 6 accessed without permission. Breaches are the result of a cyberattack where criminals gain  
 7 unauthorized access to a computer system or network and steal the private, sensitive, or confidential  
 8 personal and financial data of the customers or users contained within.

9       54.     Despite these assurances and the significant benefit Zoosk receives by collecting  
 10 and maintaining its customers' PII, Zoosk did not adopt reasonable data measures and systems to  
 11 protect customers' PII or prevent and detect unauthorized access to this data. Zoosk maintains a  
 12 business that operates exclusively online and collects hundreds of millions of dollars from online  
 13 customers each year; it has the resources to adopt reasonable protections and should have known  
 14 to do so. It knew or should have known that its systems had inadequate protections that placed its  
 15 customers at significant risk of having their PII stolen by hackers.

16       55.     Such failures resulted in the hack orchestrated by ShinyHunters on January 12, 2020  
 17 which resulted in the theft of 30 million account credentials.

18       56.     Despite its mammoth scope, Zoosk, did not become aware of the breach until May  
 19 11, 2020 – nearly four months later. Such timing coincided with media reports of the sale of such  
 20 information by ShinyHunters on the dark web for \$500 “a pop.”<sup>19</sup>

21 **Zoosk Did Not Notify Affected Consumers Within a Reasonable Time**

22       57.     Defendant also had a duty to timely discover the Data Breach and notify Plaintiffs  
 23 and Class members that their PII had been compromised. Defendant breached this duty by failing  
 24 to use reasonable intrusion detection measures to identify the Data Breach when it occurred months  
 25 prior, and then, promptly upon learning of the breach.

---

26       19 <https://www.cshub.com/attacks/articles/iotw-shiny-hunters-is-the-new-threat-actor-in-town>

58. Zoosk notified Plaintiffs and the members of the classes that personal information stolen during the breach included names, email addresses, and passwords.

**Annual Monetary Losses from Identity Theft are in the Billions of Dollars in Value of Personally Identifiable Information**

59. Zoosk's failure to implement reasonable security systems has caused Plaintiffs and Class members to suffer and continue to suffer harm that adversely impact Plaintiffs and Class members economically, emotionally, and/or socially. As discussed above, Plaintiffs and Class members now face an imminent and ongoing threat of identity theft and resulting harm. These individuals now must spend significant time and money to continuously monitor their accounts and credit scores to limit potential adverse effects of the Data Breach regardless of whether any Class member ultimately falls victim to identity theft.

60. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Experion has created the below chart tracking the sale process of the most common pieces of hacked information.<sup>20</sup>

61. Such figures are consistent with those reported by other media outlets.

62. The information stolen from Zoosk included usernames and passwords—PII that is highly valued among cyber thieves and criminals on the Dark Web. For example, Apple ID usernames and passwords were sold on average for \$15.39 each on the Dark Web, making them the most valuable non-financial credentials for sale on that marketplace. Usernames and passwords for eBay (\$12), Amazon ( $\leq \$10$ ), and Walmart ( $\leq \$10$ ) fetch similar amounts.<sup>21</sup>

63. This is particularly problematic because password reuse and modification is a very common behavior (observed on 52% of users in one study and far more in current polls).<sup>22</sup> By

<sup>20</sup> <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-sellingfor-on-the-dark-web/>

<sup>21</sup> Don Reisinger, *Here's How Much Your Stolen Apple ID Login Costs on the Dark Web*, Fortune (March 7, 2018), <https://fortune.com/2018/03/07/apple-id-dark-web-cost/>; See also <https://www.npr.org/2018/02/22/588069886/take-a-peek-inside-the-market-for-stolen-usernames-andpasswords>.

<sup>22</sup> The Next Domino To Fall: Empirical Analysis of User Passwords across Online Services Chun Wang, Steve T.K. Jan, Hang Hu, Douglas Bossart, Gang Wang. In Proceedings of The ACM

1 unlawfully obtaining this information, cyber criminals can use these credentials to access other  
 2 services beyond that which was hacked.

3       64. There may be a time lag between when harm occurs and when it is discovered, and  
 4 also between when PII is stolen and when it is used. According to the U.S. Government  
 5 Accountability Office (“GAO”), which conducted a study regarding data breaches:

6           [Law enforcement officials told us that in some cases, stolen data may be held for  
 7 up to a year or more before being used to commit identity theft. Further, once stolen  
 8 data have been sold or posted on the Web, fraudulent use of that information may  
 9 continue for years. As a result, studies that attempt to measure the harm resulting  
 10 from data breaches cannot necessarily rule out all future harm.<sup>23</sup>

11       65. As a result of the Data Breach, Plaintiffs and Class Members now face years of  
 12 constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiffs  
 13 and Class Members are also subject to a higher risk of phishing and pharming where hackers exploit  
 14 information they already obtained in an effort to procure even more PII. Plaintiff and Class Members  
 15 are presently incurring and will continue to incur such damages, in addition to any fraudulent credit  
 16 and debit card charges incurred by them, and the resulting loss of use of their credit and access to  
 17 funds, whether or not such charges are ultimately reimbursed by the credit card companies. In  
 18 addition, Plaintiff and Class Members now run the risk of unauthorized individuals creating credit  
 19 cards in their names, taking out loans in their names, and engaging in other fraudulent conduct using  
 20 their identities.

21       66. Despite this harm, Zoosk has failed to recognize the impact of the Data Breach on its  
 22 customers; it has not even offered impacted customers credit monitoring services or other mitigation  
 23 measures beyond what is available to the public. For example, Zoosk’s notice to affected customers  
 24 puts the onerous on the user to change his password and states that they “are providing the contact

---

25       26 Conference on Data and Applications Security and Privacy (CODASPY). Tempe, AZ, March  
 27 2018.

28       23 See GAO, Report to Congressional Requesters, at 33 (June 2007), *available at*  
<http://www.gao.gov/new.items/d07737.pdf>

- 1 details for the national consumer reporting agencies and a reminder to remain vigilant for incidents
- 2 for fraud and identity theft by reviewing account statements and monitoring credit reports.

3       67. Due to Defendant's conduct, Plaintiffs and Class members are entitled to credit  
4 monitoring. Credit monitoring is reasonable here. The PII taken can be used towards identity theft  
5 and other types of financial fraud against the Class members. There is no question that this PII was  
6 taken by sophisticated cybercriminals, increasing the risks to the Class members. The consequences  
7 of identity theft are serious and long-lasting. There is a benefit to early detection and monitoring.

8        68. Annual subscriptions for credit monitoring plans range from approximately \$219 to  
9        \$329 per year.

10        69. Plaintiffs and Class members therefore have a significant and cognizable interest in  
11 obtaining equitable relief (in addition to any monetary damages) that protects them from these long  
12 term threats.

## **CLASS ACTION ALLEGATIONS**

14       70. Plaintiffs bring this nationwide class action pursuant to Rule 23(b)(2), 23(b)(3), and  
15 23(c)(4) of the Federal Rules of Civil Procedure, individually and on behalf of all members of the  
16 following classes:

**17      Nationwide Class:** All individuals whose PII was compromised in the Data Breach  
18      announced by Zoosk on June 3, 2020.

**19      California Subclass:** All individuals whose PII was compromised in the Data Breach  
20     announced by Zoosk on June 3, 2020, who reside in California.

**21      Subscription Subclass:** All individuals whose PII was compromised in the Data Breach  
22      announced by Zoosk on June 3, 2020, who paid for subscriptions with Zoosk.

23        71. Specifically excluded from this Class are Defendant; the officers, directors, or  
24 employees of Defendant; any entity in which Defendant has a controlling interest; and any affiliate,  
25 legal representative, heir, or assign of Defendant. Also excluded are any federal, state, or local  
26 governmental entities, any judicial officer presiding over this action and the members of his/her  
27 immediate family and judicial staff, and any juror assigned to this action.

1       72. Plaintiffs reserve the right to modify or amend the definition of the proposed Class  
 2 before the Court determines whether certification is appropriate.

3       73. **Numerosity:** The Classes are sufficiently numerous, as each includes hundreds of  
 4 thousands of individuals. According to the Notice provided by Zoosk, there are 560,138 California  
 5 residents affected. Thus, joinder of such persons in a single action or bringing all members of the  
 6 Classes before the Court is impracticable for purposes of Rule 23(a)(1).

7       74. The question is one of a general or common interest of many persons and it is  
 8 impractical to bring them all before the Court. The disposition of the claims of the members of the  
 9 Classes in this class action will substantially benefit both the parties and the Court.

10      75. **Commonality:** There are questions of law and fact common to each Class for  
 11 purposes of Rule 23(a)(2), including:

- 12           a. Whether and when Defendant actually learned of the data breach and whether  
                 its response was adequate;
- 13           b. Whether Defendant owed a duty to the Class to exercise due care in collecting,  
                 storing, safeguarding and/or obtaining their PII;
- 14           c. Whether Defendant breached that duty;
- 15           d. Whether Defendant implemented and maintained reasonable security procedures  
                 and practices appropriate to the nature of storing Plaintiffs' and Class members'  
                 PII;
- 16           e. Whether Defendant acted negligently in connection with the monitoring  
                 and/or protecting of Plaintiff's and Class members' PII;
- 17           f. Whether Defendant knew or should have known that it did not employ reasonable  
                 measures to keep Plaintiffs' and Class members' PII secure and prevent loss or  
                 misuse of that PII;
- 18           g. Whether Defendant adequately addressed and fixed the vulnerabilities which  
                 permitted the data breach to occur;

- h. Whether Defendant caused Plaintiffs and Class members damages, including compensatory, statutory, actual, consequential, or nominal damages;
  - i. Whether Defendant violated the law by failing to promptly notify class members that their PII had been compromised;
  - j. Whether Plaintiffs and the other Class members are entitled to credit monitoring and other monetary relief;
  - k. Whether Plaintiffs and Class members are entitled to compensatory, statutory, actual, consequential, or nominal damages, credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendant’s wrongful conduct; and
  - l. Whether Defendant violated California’s Deceptive and Unfair Trade Practices Act by failing to implement reasonable security procedures and practice.

12        76.     **Typicality:** Plaintiffs assert claims that are typical of the claims of each respective  
13 Class for purposes of Rule 23(a)(3). Plaintiffs and all members of each respective Class have had  
14 their PII compromised as a result of the data breach and Defendant's misconduct.

15        77.     **Adequacy:** Plaintiffs will fairly and adequately represent and protect the interests  
16 of the other members of each respective Class for purposes of Rule 23(a)(4). Plaintiffs have no  
17 interests antagonistic to those of other members of each respective Class. Plaintiffs are committed  
18 to the vigorous prosecution of this action and has retained counsel experienced in litigation of this  
19 nature to represent her. Plaintiffs anticipate no difficulty in the management of this litigation as a  
20 class action.

21       78. Class certification is appropriate under Rule 23(b)(2) because Defendant has acted  
22 on grounds that apply generally to each Class, so that final injunctive relief or corresponding  
23 declaratory relief is appropriate respecting each Class as a whole.

24        79. Class certification is appropriate under Rule 23(b)(3) because common questions of  
25 law and fact substantially predominate over any questions that may affect only individual members  
26 of each Class.

80. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by the members of each respective Class. Similar or identical statutory and common law violations and deceptive business practices are involved. Individual questions, if any, pale by comparison to the numerous common questions that predominate.

81. The injuries sustained by Plaintiffs and the members of each Class flow, in each instance, from a common nucleus of operative facts – Defendant’s misconduct.

82. Plaintiffs and the members of each Class have been damaged by Defendant's misconduct.

9        83. Proceeding as a class action provides substantial benefits to both the parties and the  
10 Court because this is the most efficient method for the fair and efficient adjudication of the  
11 controversy. Members of each Class have suffered and will suffer irreparable harm and damages as  
12 a result of Defendant's wrongful conduct. Because of the nature of the individual claims of the  
13 members of each Class, few, if any, could or would otherwise afford to seek legal redress against  
14 Defendant for the wrongs complained of herein, and a representative class action is therefore the  
15 appropriate, superior method of proceeding and essential to the interests of justice insofar as the  
16 resolution of claims of the members of each Class is concerned. Absent a representative class action,  
17 members of each Class would continue to suffer losses for which they would have no remedy, and  
18 Defendant would unjustly retain the proceeds of its ill-gotten gains. Even if separate actions could  
19 be brought by individual members of each Class, the resulting multiplicity of lawsuits would cause  
20 undue hardship, burden, and expense for the Court and the litigants, as well as create a risk of  
21 inconsistent rulings, which might be dispositive of the interests of the other members of each Class  
22 who are not parties to the adjudications and/or may substantially impede their ability to protect their  
23 interests.

24        84. Particular issues under Rule 23(c)(4) are appropriate for certification because such  
25 claims present only particular, common issues, the resolution of which would advance the  
26 disposition of this matter and the parties' interests therein. Such particular issues include, but are  
27 not limited to:

- 1 a. Whether Defendant owed a legal duty to Plaintiffs and the Class members to  
2 exercise due care in collecting, storing, using, and safeguarding their PII;
- 3 b. Whether Defendant breached a legal duty to Plaintiffs and the Class members  
4 to exercise due care in collecting, storing, using, and safeguarding their PII;
- 5 c. Whether Defendant failed to comply with its own policies and applicable laws,  
6 regulations, and industry standards relating to data security;
- 7 d. Whether Defendant failed to implement and maintain reasonable security  
8 procedures and practices appropriate to the nature and scope of the information  
9 compromised in the data breach; and
- 10 e. Whether Class members are entitled to compensatory, statutory, actual,  
11 consequential, or nominal damages, credit monitoring or other injunctive relief,  
12 and/or punitive damages as a result of Defendant's wrongful conduct.

**FIRST CAUSE OF ACTION**

**NEGLIGENCE**

**(By Plaintiffs and the Classes)**

15 85. Plaintiffs re-allege and incorporate by reference herein all of the allegations  
16 contained in paragraphs 1 through 84 above.

17 86. Defendant owed Plaintiffs and Class members a duty to exercise reasonable care in  
18 protecting their PII from unauthorized disclosure or access. Defendant breached its duty of care by  
19 failing to implement reasonable security procedures and practices to protect Plaintiffs' and Class  
20 members' PII. Defendant failed to, inter alia: (i) implement security systems and practices consistent  
21 with federal and state guidelines; (ii) implement security systems and practices consistent with  
22 industry norms; (iii) timely detect the Data Breach; and (iv) timely disclose the Data Breach to  
23 impacted customers.

24 87. Additionally, Defendant collected money from the Subscription Subclass but failed  
25 to commit appropriate portions of that money to enact security measures to protect Plaintiffs' and  
26 Class Members' PII.

1       88.     Defendant knew or should have known Plaintiffs' and Class members' PII was highly  
 2 sought after by hackers and that Plaintiffs and Class members would suffer significant harm if their  
 3 PII was stolen by hackers.

4       89.     Defendant also knew or should have known that timely disclosure of the Data Breach  
 5 was required and necessary to allow Plaintiffs and Class members to take appropriate actions to  
 6 mitigate the resulting harm. These efforts include, but are not limited to, freezing accounts, changing  
 7 passwords, monitoring credit scores/profiles for fraudulent charges, contacting financial institutions,  
 8 and cancelling or monitoring government-issued IDs such as passports and driver's licenses. The  
 9 risk of significant harm to Plaintiffs and Class members (including identity theft) increased as the  
 10 amount of time between the Data Breach and disclosure lengthened to reach a full twenty-two days.

11      90.     Defendant had a special relationship with Plaintiffs and the Class members who  
 12 entrusted Defendant with several pieces of PII. Customers were required to provide PII when  
 13 utilizing Defendant's properties and/or services. Plaintiffs and Class members were led to believe  
 14 Defendant would take reasonable precautions to protect their PII and would timely inform them if  
 15 their PII was compromised, but the Defendant did not do so.

16      91.     Defendant's duty to use reasonable data security measures also arose under Section  
 17 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45(a).

18      92.     The Federal Trade Commission ("FTC") has established security guidelines and  
 19 recommendations to help entities protect PII and reduce the likelihood of data breaches.

20      93.     Specifically, Section 5 of the FTC Act, 15 U.S.C. § 45(a), prohibits "unfair ...  
 21 practices in or affecting commerce," including, as interested and enforced by the FTC, the unfair  
 22 practices of failing to use reasonable measures to protect PII by companies such as Defendant.

23      94.     Various FTC publications and data security breach orders further form the basis of  
 24 Defendant's duty.<sup>24</sup> Plaintiffs and Class members are consumers under the FTC Act. Defendant  
 25

---

26      24 See, e.g., Data Protection: Actions taken by Equifax and Federal Agencies in Response to the  
 27 2017 Breach, United States Government Accountability Office (Aug. 30, 2019), available at:  
<https://www.gao.gov/products/GAO-18-559> (regarding the Equifax data breach).

1 violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not  
 2 complying with industry standards.

3       95. In addition, Cal. Civ. Code § 1798.81.5 requires Defendant to take reasonable steps  
 4 and employ reasonable methods of safeguarding the PII of Class members who are California  
 5 residents.

6       96. Defendant violated the FTC Act and the CCPA by failing to use reasonable security  
 7 measures to protect PII and not complying with applicable industry, federal, and state guidelines  
 8 and standards. Defendant's conduct was particularly unreasonable given the nature and amount of  
 9 customer PII it stored and the foreseeability and resulting consequences of a data breach.

10      97. Plaintiffs and Class members are part of the Class of persons the FTC Act and CCPA  
 11 were intended to protect. The harm that was proximately caused by the Data Breach is the type of  
 12 harm the FTC Act and CCPA were intended to guard against. The FTC has brought enforcement  
 13 actions against entities that, due to a failure to employ reasonable data security measures, caused  
 14 the same harm as that suffered by Plaintiffs and Class members here.

15      98. As a result of Defendant's negligence, Plaintiffs and Class members suffered injuries  
 16 that may include: (i) the lost or diminished value of PII; (ii) out-of-pocket expenses associated with  
 17 the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of  
 18 their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences  
 19 of the data breach, including but not limited to time spent deleting phishing email messages and  
 20 cancelling credit cards believed to be associated with the compromised account; (iv) the continued  
 21 risk to their PII, which remains for sale on the dark web and is in Defendant's possession, subject  
 22 to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate  
 23 measures to protect the PII of customers and former customers in its continued possession; (v) future  
 24 costs in terms of time, effort, and money that will be expended to prevent, monitor, detect, contest,  
 25 and repair the impact of the PII compromised as a result of the data breach for the remainder of the  
 26 lives of Plaintiffs and Class members, including ongoing credit monitoring.

27

28

99. The harm that Plaintiffs and Class members suffered (and continue to suffer) was the reasonably foreseeable product of Defendant's breach of its duty of care. Defendant failed to enact reasonable security procedures and practices and Plaintiffs and Class members were the foreseeable victims of data theft that exploited the inadequate security measures. The PII accessed in the Data Breach is precisely the type of information that hackers seek and use to commit cyber crimes.

## **SECOND CAUSE OF ACTION**

**VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW  
CAL. BUS. & PROF. CODE § 17200 – UNFAIR BUSINESS PRACTICES  
(By Plaintiff Flores-Mendez and the Subscription Subclass)**

9       100. Plaintiff Flores-Mendez re-alleges and incorporates by reference herein all of the  
allegations contained in paragraphs 1 through 84 above.  
10

11        101. Defendant's conduct as alleged herein constitutes unfair, and/or fraudulent business  
12 acts or practices as prohibited by the UCL.

13        102. “Unfair” acts under the UCL have been interpreted using three different tests: (1)  
14              whether the public policy which is a predicate to a consumer unfair competition action under the  
15              unfair prong of the UCL is tethered to specific constitutional, statutory, or regulatory provisions; (2)  
16              whether the gravity of the harm to the consumer caused by the challenged business practice  
17              outweighs the utility of the defendant’s conduct; and (3) whether the consumer injury is substantial,  
18              not outweighed by any countervailing benefits to consumers or competition, and is an injury that  
19              consumers themselves could not reasonably have avoided. Defendant’s conduct is unfair under each  
20              of these tests.

21        103. Defendant engaged in business acts or practices deemed “unfair” under the UCL  
22 because, as alleged above, Defendant failed to disclose the inadequate nature of the security of its  
23 computer systems and networks that stored Plaintiff’s and the Subscription Subclass members’  
24 sensitive PII. *See* Cal. Bus. & Prof. Code § 17200.

25       104. Additionally, Defendant collected money from the Subscription Subclass but failed  
26 to commit appropriate portions of that money to enact security measures to protect Plaintiffs' and  
27 Class Members' PII.

1       105. Defendant's conduct was also unfair because it failed to use reasonable security  
 2 measures to protect Plaintiffs' and Class Members' PII.

3       106. Defendant's conduct violates the policies of the statutes referenced above. Moreover,  
 4 Defendant's conduct is contrary to public policy, immoral, unethical, oppressive, unscrupulous  
 5 and/or substantially injurious to consumers. Among other things, it is contrary to the public policy  
 6 in favor of protecting consumer data.

7       107. The gravity of the harm of Defendant's failure to secure and protect Plaintiffs' and  
 8 Class Members' sensitive PII is significant and there is no corresponding benefit resulting from such  
 9 conduct. Finally, because Plaintiffs and Class Members were completely unaware of Defendant's  
 10 inadequate information security practices, they could not have avoided the harm resulting from  
 11 Defendant's conduct.

12       108. Had Plaintiff Flores-Mendez known that his PII would not be adequately secured and  
 13 protected, he would not have used Defendant's services. Plaintiffs and Class Members have a  
 14 property interest in their sensitive PII. By failing to adequately secure and protect that sensitive PII,  
 15 Defendant has taken property from Plaintiffs and Class Members without providing just or any  
 16 compensation.

17       109. Plaintiff Flores-Mendez and the Subscription Subclass members have lost money  
 18 and property as a result of Defendant's conduct in violation of the UCL and seek restitution on  
 19 behalf of himself and the Subscription Subclass Members. Additionally, Plaintiff Flores-Mendez  
 20 individually and on behalf of the Class, seeks an injunction enjoining Defendant from engaging in  
 21 the unlawful conduct alleged in this claim and requiring Defendant to delete Plaintiffs' and Class  
 22 members' sensitive PII, to cease further collection of Plaintiffs' and Class members' sensitive PII,  
 23 and other appropriate equitable relief, including but not limited to implementing adequate  
 24 information security policies and practices.

25       ///

26       ///

27       ///

## PRAAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the Classes, request the following relief:

1. A determination that this action is a proper class action under Federal Rule of Civil Procedure 23, certifying the Classes, and appointing Plaintiffs as Class Representatives and their counsel as Class Counsel;
  2. Finding that Defendant's conduct was unlawful as alleged herein;
  3. An award of compensatory, punitive, statutory, actual, consequential, or nominal damages or civil penalties to Plaintiffs and the Classes as warranted by applicable law;
  4. An order requiring Defendant to purchase or provide funds for credit monitoring services for Plaintiffs and all Class Members;
  5. An award of injunctive or other equitable relief that directs Defendant to implement adequate security procedures and practices to protect customers' PII that conform to relevant federal and state guidelines and industry norms;
  6. Awarding Plaintiffs and the Class reasonable costs and expenses incurred in this action, including attorneys' fees, costs, and expenses, including expert fees;
  7. Awarding Plaintiffs and the Class Members pre- and post-judgment interest; and
  8. Such other relief as the Court may deem just and proper.

Dated: February 17, 2022

**BRADLEY/GROMBACHER, LLP**

By: /s/ Kiley L .Grombacher  
Marcus J. Bradley, Esq.  
Kiley L. Grombacher, Esq.  
Lirit A. King, Esq.  
31365 Oak Crest Drive Suite 240  
Westlake Village, CA 91361  
Telephone: (805) 270-7100  
Facsimile: (805) 270-7589  
Email: mbradley@bradleygrombacher.com  
kgrombacher@bradleygrombacher.com  
lking@bradleygrombacher.com

**BRADLEY/GROMBACHER, LLP**  
Robert N. Fisher (SBN 302919)  
477 Madison Avenue, Suite 6000  
New York, NY 10022  
Telephone: (805) 270-7100  
E-Mail: [rfisher@bradleygrombacher.com](mailto:rfisher@bradleygrombacher.com)

**CROSNER LEGAL P.C.**  
Zachary M. Crosner (SBN 272295)  
Michael R. Crosner (SBN 41299)  
433 N. Camden Dr., Suite 400  
Beverly Hills, CA 90210  
Telephone: (310) 496-4818  
Facsimile: (310) 510-6429  
Email: [zach@crosnerlegal.com](mailto:zach@crosnerlegal.com)  
[mike@crosnerlegal.com](mailto:mike@crosnerlegal.com)

**MORGAN & MORGAN  
COMPLEX LITIGATION GROUP**  
John A. Yanchunis (*admitted pro hac vice*)  
Ryan McGee (*admitted pro hac vice*)  
201 N Franklin St., 7th Floor  
Tampa, FL 33602  
Telephone: (813) 223-5505  
Email: [jyanchunis@forthepeople.com](mailto:jyanchunis@forthepeople.com)  
[rmcgee@forthepeople.com](mailto:rmcgee@forthepeople.com)

*Attorneys for Plaintiffs*

## **DEMAND FOR JURY TRIAL**

Plaintiffs hereby demand a jury trial for all claims so triable.

Dated: February 17, 2022

## **BRADLEY/GROMBACHER, LLP**

By: /s/ Kiley L .Grombacher  
Marcus J. Bradley, Esq.  
Kiley L. Grombacher, Esq.  
Lirit A. King, Esq.  
31365 Oak Crest Drive Suite 240  
Westlake Village, CA 91361  
Telephone: (805) 270-7100  
Facsimile: (805) 270-7589  
Email: mbradley@bradleygrombacher.com  
kgrombacher@bradleygrombacher.com  
lkling@bradleygrombacher.com

**BRADLEY/GROMBACHER, LLP**  
Robert N. Fisher (SBN 302919)  
477 Madison Avenue, Suite 6000  
New York, NY 10022  
Telephone: (805) 270-7100  
E-Mail: [rfisher@bradleygrombacher.com](mailto:rfisher@bradleygrombacher.com)

**CROSNER LEGAL P.C.**  
Zachary M. Crosner (SBN 272295)  
Michael R. Crosner (SBN 41299)  
433 N. Camden Dr., Suite 400  
Beverly Hills, CA 90210  
Telephone: (310) 496-4818  
Facsimile: (310) 510-6429  
Email: [zach@crosnerlegal.com](mailto:zach@crosnerlegal.com)  
[mike@crosnerlegal.com](mailto:mike@crosnerlegal.com)

**MORGAN & MORGAN  
COMPLEX LITIGATION GROUP**  
John A. Yanchunis (*admitted pro hac vice*)  
Ryan McGee (*admitted pro hac vice*)  
201 N Franklin St., 7th Floor  
Tampa, FL 33602  
Telephone: (813) 223-5505  
Email: [jyanchunis@forthepeople.com](mailto:jyanchunis@forthepeople.com)  
[rmcghee@forthepeople.com](mailto:rmcghee@forthepeople.com)

*Attorneys for Plaintiffs*